



⑬ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑫ **Offenlegungsschrift**
⑩ **DE 197 12 053 A 1**

⑳ Aktenzeichen: 197 12 053.9
㉔ Anmeldetag: 23. 3. 97
㉕ Offenlegungstag: 24. 9. 98

⑤ Int. Cl.⁶:
G 07 C 9/00
H 04 B 1/38
H 04 L 9/32
G 08 B 13/22
G 08 B 29/00

DE 197 12 053 A 1

㉑ Anmelder:
Baltus, René, 53125 Bonn, DE

㉒ Erfinder:
Baltus, Rene, 53125 Bonn, DE; Woop, Marc-Bernd,
53111 Bonn, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

⑤④ Kommunikationsgeräte mit Vorrichtungen zur Aufnahme biometrischer Merkmale

⑤⑦ Die Erfindung betrifft die Kombination von Kommunikationsgeräten, auch portable, mit Vorrichtungen zur Erfassung und dem Vergleich von biometrischen Merkmalen. Der Ersatz von gefährdeten Codes und PIN durch biometrische Identifikation wie z. B. vierdimensionale on line Schriftprüfung, soll die Sicherheit im allgemeinen Datenverkehr mit Telefon, Telefax, Funk, etc., aber auch beim Teleshopping und Telebanking erhöhen.

DE 197 12 053 A 1

BEST AVAILABLE COPY

Beschreibung

Kommunikationsgeräte wie Telefone, Funkgeräte, Faxgeräte, etc. sind im allgemeinen bekannt. Sie werden vielfältig eingesetzt und erfreuen sich steigender Beliebtheit. Diese Geräte werden in stationären und tragbaren Ausführungen angeboten. Weiterhin sind die einzelnen Geräte in verschiedenen Kombinationen auf dem Markt.

Die allgemein steigenden Bedürfnisse nach Kommunikation und die vielfältigen Aufgaben die fernmündlich und fernschriftlich über Draht und Funk getätigt werden (z. B. Teleshopping, Telebanking) erfordern einen immer höheren Sicherheitsstandard um unbefugtes Abhören und Nutzen zu verhindern. Besonders die Authentikation der einzelnen Teilnehmer kann hierzu einen Beitrag leisten. Diese Authentikation erfolgt bisher hauptsächlich mit Codes oder persönlichen Identifikationsnummern, sogenannten PIN. Selbst die "digitale Signatur" erfordert eine PIN um die auf einer Smartcard gespeicherten Identifikationsalgorithmen zu starten und auszuführen. Bei PIN und Codes wird aber nur Wissen und nicht persönliche Eigenschaften abgefragt!

PIN und Codes können sehr gut verschlüsselt werden. Wird von der Annahme ausgegangen, daß die Verschlüsselungen von Unbefugten nicht zu entschlüsseln sind (viele Fachleute sind sich nicht so sicher), bleibt die Gefahr, daß die Nutzer nicht richtig mit dem Paßwort umgehen können. Wie Claus Schönleber in seinem Buch "Verschlüsselungsverfahren für PC" (Franzis Verlag 1996) bemerkt: "... der menschliche Faktor ist das Problem" Weiter: "Wenn ich mit meinem Paßwort nicht richtig umgehen kann, wenn mir meine Identifikation gestohlen wird (oder erpreßt, oder fahrlässig weitergegeben wird) oder wenn ich meine Identifikation zu unsicher aufbewahre, dann mache ich jedes Sicherheitssystem zunichte".

Aus den vorgenannten Gründen bietet sich an, die oben erwähnten Kommunikationsgeräte mit Vorrichtungen auszustatten, die eine Identifikation durch biometrische Merkmale zulassen. Hierzu zählen Geräte zur Gesichtserkennung, zur Erkennung der Finger- und Stimmabdrücke, zur Erkennung der Hand und Fingerform. Weiterhin sind Geräte zur Schrifterkennung bekannt.

Diese Vorrichtungen waren bisher sehr teuer und benötigten viel Raum oder im Falle der Schrifterkennung, den Einsatz von Spezialstiften. Ein Einbau in kleine und sogar tragbare Geräte ist für den Masseneinsatz zu einem vertretbarem Preis kaum möglich.

Die Erfindung hat sich zur Aufgabe gestellt, diese Nachteile zu beseitigen und Kommunikationsgeräte mit einer oder mehreren Vorrichtungen zur Aufnahme von biometrischen Merkmalen auszurüsten.

Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß eine Kombination von Kommunikationsgeräten, wie Telefone, tragbare Telefone (Handy), Funkgeräte, Telefaxgeräte, etc. mit einer Vorrichtung zum Erfassen von Unterschriften wie z. B. in EP 0 560 356 B1 und weiteren Anmeldungen beschrieben, der Erfassung der Pausenzeiten beim Nutzen der Tastatur und der Erfassung der Stimmfrequenz hergestellt wird. Werden in absehbarer Zeit CCD-Kameras in Kleinformat zur Verfügung stehen, sind diese ebenfalls einsetzbar. In bekannten und geeigneten elektronischen Schaltungen und Programmen werden die erfaßten biometrischen Merkmale mit hinterlegten oder in geeigneter Form, z. B. auf Plastikkarten mit Chip oder Magnetstreifen, gespeicherten Mustern verglichen. Bei Übereinstimmung erfolgt eine Freigabe, bei Nichtübereinstimmung erfolgt eine Sperrung von Funktionen.

Wird ein Kommunikationsgerät mit einer Vorrichtung zur Erfassung von biometrischen Merkmalen kombiniert, sind

vielfältige Funktionen möglich.

Ein abgesandtes Fax, z. B. erhält einen wesentlich höheren juristisch durchsetzbaren Wert. Weiterhin kann niemand außer dem Berechtigten beim Telebanking oder Teleshopping mittels Fernsprechgeräten einen Auftrag ausführen oder sonstige Geschäfte tätigen. Besonders die immer mehr in Mode kommenden sogenannten "Handys" werden durch die vorgeschlagene Verbesserung erheblich aufgewertet. Somit sind jederzeit und von jedem Ort aus alle Geschäfte mit einer biometrischen Identifikation, z. B. einer Unterschrift, abzuschließen.

Werden die Transaktionen mit einer echten, vierdimensional erfaßten Signatur abgeschlossen, kommt dies praktisch einer auf Papier getätigten Unterschrift gleich. Nach wie vor gilt: "Die Unterschrift als Ausdruck einer Handlung 'mit seinem Namen für etwas stehen' hat nach wie vor große Bedeutung im Rechtsleben. Ihr schrieb man nicht nur in der Vergangenheit individuelle Unverwechselbarkeit zu; auch heute, in einem hochtechnisierten Zeitalter wird der persönlichen Namenszeichnung ein hoher Identifikationswert beigemessen" (Forensische Schriftprüfung, Seite 238, M. Hekker, Kriminalistik Verlag, Wiesbaden, 1993).

Wird die vorgenannte Maßnahme mit einer weiteren Erfassung von biometrischen Merkmalen, wie z. B. Stimmabdruck oder Pausenzeiten, erweitert, ist eine Fälschung kaum denkbar. Die Gefahr der Ablehnung des Berechtigten verringert sich auf theoretische Werte.

Eine weitere vorteilhafte Nutzung des Schriftenprüfers liegt darin, daß eine geleistete Unterschrift oder ein geschriebener Code als Zufallsgenerator für einen Verschlüsselungsalgorithmus herangezogen werden kann. Dies geschieht auf gleicher Weise, wie im Verschlüsselungsverfahren Pretty Good Privacy "PGP" von Zimmermann genutzt.

Da die auf die Schreibunterlage ausgeübten Drücke, bzw. die Druckpunkte jederzeit bekannt sind, kann der Schriftprüfer gleichzeitig als Tastatur verwendet werden. Hierdurch können alle oder teilweise die Wahl- und Funktionstasten der Kommunikationsgeräte eingespart werden. Zur Nutzung als Tastatur werden die einzelnen Tastenfelder zur sicheren Bedienung und um Fehl tastungen auszuschließen mit einer Fuzzy-Logik zentriert.

Patentansprüche

1. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen, dadurch gekennzeichnet, daß die Geräte fest angebrachte und integrierte oder beigestellte Vorrichtungen (Hard- und Software) zur Aufnahme, Speicherung und Vergleich von biometrischen Merkmalen, z. B. von Schriftdrücken, Stimmfrequenzen, der Pausenzeiten beim Nutzen der Tastatur, Gesichtserkennung und Fingerabdrücken oder eine beliebige Kombination der einzelnen Vorrichtungen erhalten und diese eine gegenseitige Authentikation mit anderen Nutzern von Kommunikationsgeräten erlauben.

2. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach Anspruch 1, dadurch gekennzeichnet, daß ein Schriftprüfer wie in EP 0 560 356 B1 beschrieben und der mit einer Fuzzylogik zur sicheren Findung und Erkennung der Tasten ausgestattet ist, gleichzeitig als Tastenfeld zur Wahl von Kommunikationszielen sowie anderen gerätespezifischen Funktionen und als Unterschriftenprüfer für Normalstifte genutzt wird.

3. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, daß die

biometrischen Merkmale des Berechtigten verschlüsselt auf einem Datenspeicher wie Magnetstreifen oder Chip (Smartchip) einer Benutzerkarte wie z. B. der üblichen Karten zum Freischalten der Handtelefone (Handy) oder Scheck-, Geld- oder Kreditkarten gespeichert und auf Abruf zur Verfügung stehen. 5

4. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, daß das aufgenommene biometrische Merkmal verschlüsselt, vorausgesendet, überprüft und bei Übereinstimmung zur Öffnung einer berechtigten Verbindung oder Datei oder Fernbedienung von Systemen und Geräten der angewählten Gegenseite genutzt wird. Nichtübereinstimmung signalisiert einen unberechtigten Einbruchversuch und führt zu Sperrungen oder Alarmen. 15

5. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, daß das aufgenommene biometrische Merkmal nachgesendet und überprüft wird und bei Übereinstimmung und zu einem gewünschten und berechtigten Abschluß der Tätigkeit z. B. einer geschäftlichen oder finanziellen Transaktion führt. Nichtübereinstimmung signalisiert einen unberechtigten Einbruchversuch und führt zu Abbrüchen, Sperrungen oder Alarmen. 25

6. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 5, dadurch gekennzeichnet, daß das aufgenommene biometrische Merkmal vor seiner Über- 30 sendung an die Gegenstelle verschlüsselt und/oder mit einem verborgenen Zeitstempel versehen wird.

7. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, daß die Aufnahme des biometrischen Merkmals durch einen programm eigenen Lernvorgang erfolgt und das Programm ein Kennfeld erstellt in dessen Grenzen sich später die Abweichungen der biometrischen Merkmale bewegen dürfen ohne daß eine unnötige Ablehnung des Berechtigten erfolgt. 35

8. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, daß die Aufnahme des biometrischen Merkmals durch einen programm eigenen Lernvorgang erfolgt und das Programm ein Kennfeld erstellt, das einstellbar ist und das selbsttätig entscheidet, wann ein ungeübter Berechtigter eine genügend fälschungssichere (schmale) Kennfeldstruktur erreicht hat und dieses Ergebnis dem Berechtigten 45 mitteilt.

9. Kommunikationsgeräte mit Vorrichtungen zur Aufnahme von biometrischen Merkmalen nach den Ansprüchen 1 bis 8, dadurch gekennzeichnet, daß eine geleistete Unterschrift, ein geschriebener Code, ggfs. in Verbindung mit anderen Werten aus biometrischen Merkmalen, wie z. B. die Pausenzeiten beim Benutzen der Tastatur, als Zufallsgenerator für einen Verschlüsselungsalgorithmus herangezogen werden. 50

60

65

- Leerseite -

BEST AVAILABLE COPY